JURIDIQUE

Protection des données personnelles

L'incontournable RSSI

La mise en conformité des entreprises devrait associer de façon pérenne le RSSI au Délégué à la Protection des Données autour des mêmes principes de gestion de risques.

Les auteurs

Eric A. CAPRIOLI,
Avocat à la Cour, Docteur en droit, Vice-Président du CESIN.

Isabelle CANTERO, *Juriste senior, Responsable du Pôle Données personnelles et vie privée (Caprioli & Associés, société d'avocats).*

Les évolutions technologiques pourraient aisément faire l'objet d'une liste à la Prévert mais, outre leur volume et leur variété, c'est aussi leur large diffusion qui retient l'attention puisqu'elles concernent indifféremment le « grand public » et les entreprises, quelle que soient leur taille ou le secteur d'activités. Médias sociaux, Big data, externalisation en mode Saas / Cloud computing, objets connectés, Web 3.0... font donc désormais partie de l'environnement technique certes, mais également social, économique, et juridique (et demain fiscal[1]...) des personnes physiques (individus) ou morales (sociétés et collectivités publiques).

Concrètement, l'extension de la sphère numérique a contribué au développement exponentiel de la collecte et du traitement des données à caractère personnel, lesdites données étant constitutives de nouvelles opportunités économiques pour nombre d'entreprises et, dans tous les cas, un patrimoine informationnel à valoriser et à protéger.

Pour rappel, les données personnelles présentent la particularité de faire l'objet d'une protection spécifique dans tous les Etats de l'Union européenne suite à leur transposition de la directive 95/46 et dans les Etats membres du Conseil de l'Europe (47 états membres et 6 observateurs)[2], mais non membres de l'Union européenne comme Monaco, la fédération de Russie ou la Turquie. Est-ce à dire, au niveau de l'entreprise, que l'application de la règlementation sur la protection des données à caractère personnel est du seul ressort du juriste ? Rien n'est moins sûr, et la refonte du cadre réglementaire européen[3] en atteste. De fait, les Responsables de la sécurité des Systèmes d'information (RSSI) doivent prendre en compte des risques accrus (intrusion, divulgation, atteinte à la réputation, altération/perte de données, traitements non autorisés, etc.) et, en matière de données personnelles, les exigences prescrites au titre de la sécurité militent en faveur d'une nécessaire coopération en interne, en particulier avec le Correspondant à la Protection des Données (futur Délégué à la Protection des Données - DPD), dès lors que le RSSI n'endosse pas cette fonction.

La multiplicité des exigences légales et réglementaires (en ce compris les positions de la CNIL en France et du G29 pour l'Union européenne) complexifie la mise en conformité des entreprises et devrait associer de façon pérenne le RSSI au DPD autour des mêmes principes de gestion de risques et ainsi garantir leurs process de protection des traitements de données à caractère personnel.

A l'instar du système espagnol actuel (qui place les RSSI, dont la désignation est obligatoire pour les traitements à risque, sous la responsabilité de l'Autorité de protection des données), la future règlementation européenne met la sécurité des données au premier plan des exigences de protection.

Sécurité et obligation de notification des violations des données personnelles

En droit français, le principe général de sécurité et de confidentialité des données à caractère personnel est établi à l'article 34 de la loi « Informatique et Libertés » de 1978, mod. 2004. En vertu de celui-ci, le responsable de traitement est tenu de *«prendre toutes les précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité*

---

[1] Rapport d'information sur le développement de l'économie numérique française, déposé par la Commission des Affaires économiques, présenté par Mmes Corinne ERHEL et Laure de LA RAUDIÈRE, enregistré à la Présidence de l'Assemblée nationale le 14 mai 2014.
Rapport du Comité d'Experts européen du 28 mai 2014 relatif à la fiscalité de l'économie digitale.

[2] V. le site : http://hub.coe.int/fr/

[3] Proposition de règlement européen sur la protection des données : Commission européenne version du 25/01/2012 et Résolution législative du Parlement européen du 12 mars 2014.

des données et notamment d'empêcher que les données soient déformées, endommagées, ou que des tiers non autorisés y aient accès ». Pour rappel, ce principe existe depuis l'adoption de la loi en 78 (sous l'article 29, étant noté que la formulation est reprise à l'identique par l'actuel article 34) et figure dans la directive européenne de 1995.

D'un point de vue opérationnel, pour garantir la sécurité et la confidentialité des données personnelles, les entreprises disposent d'une grande latitude qui variera selon l'état de l'art et en fonction du niveau de sensibilité des données ou du niveau de risque des traitements concernés. Ceci étant, il convient d'oublier la version laconique de l'actuel article 34, le nouvel article 30 de la proposition de Règlement indiquant les éléments et principes de la politique de sécurité à adopter par le responsable de traitement, la liste étant pour le moins détaillée et présumée non exhaustive.

C'est dans ce contexte « sécuritaire » que le RSSI comme le DPD doivent également se préparer à répondre à la nouvelle obligation de notification des violations de données à caractère personnelles. Très récemment, la presse s'est faite l'écho de violations de données (par deux fois pour Orange), l'obligation de notification prescrite par l'article 34 bis de la loi « Informatique et Libertés » ayant vocation à s'appliquer exclusivement aux fournisseurs de services de communications électroniques sur les réseaux de communications électroniques ouverts au public, c-à-d aux opérateurs ainsi qu'aux FAI. Les clients de l'opérateur ont été notifiés par voie de courrier électronique. La proposition de Règlement européen sur la protection des données à caractère personnel étend l'obligation de notification des violations de données à tous les responsables de traitement. Il en ira sans doute de même en France dans le cadre du projet de loi numérique.

Si d'aucuns en doutaient, la sécurité des données doit être considérée comme une obligation de résultat. En effet, outre le préjudice d'image et les coûts engendrés par les notifications aux clients concernés par une violation, il est également important de garder à l'esprit qu'en cas de manquement, des sanctions financières sont prévues (chiffrées en million d'euros et en pourcentage du CA mondial annuel dans la Proposition de règlement européen) et pourquoi pas des actions de groupe depuis la loi Hamon de 2014 ? Concernant les notifications des atteintes aux données personnelles et des failles de sécurité, les textes en préparation (propositions de Directive sécurité des réseaux et DSP2, Décrets de la Loi de programmation militaire) ou récemment adopté (Règlement EiDas du 23 juillet 2014) imposent de réunir dès à présent les différents acteurs concernés (RSSI, Correspondant à la protection des données, juridique, communication, etc.) afin d'élaborer les procédures adaptées permettant de faire face à ces obligations. Il résultera de ces nouvelles dispositions une sécurisation accrue des données personnelles qui sera toujours à renforcer en fonction de l'évolution des risques. Cela conduira l'entreprise à organiser les procédures de détection des incidents, de sorte qu'elle soit en capacité de réagir conformément aux prescriptions légales. Elle devra assurer le suivi interne des violations, pour les activités concernées par la notification. Le RSSI devra trouver les solutions adaptées, comme le contingentement des traitements, pour éviter une augmentation démesurée du champ de la notification en cas d'incident, ou procéder à l'anonymisation irrémédiable des données ou encore en utilisant des moyens de chiffrement.

Ces dispositions placent la sécurité au cœur des problématiques de protection des données et confèrent au RSSI un rôle clé. Sur un plan opérationnel, les processus de protection doivent être transverses et s'appuyer sur des compétences complémentaires permettant de maîtriser les aspects juridiques et techniques. Le système de Management de la sécurité de l'information (ISO 27001), déjà utilisés par les RSSI, pourrait être appliqué aux traitements des données personnelles afin de répondre aux exigences légales, en ce inclus la notification des violations de données à l'autorité de contrôle. L'analyse de risques doit permettre de sélectionner les mesures de sécurité du SI (sauvegardes, sécurités des accès logiques et physiques, cloisonnement des traitements ...) et la documentation y afférente, de fournir rapidement les informations nécessaire à tout contrôle ou correctifs (descriptif des mesures dont le chiffrement, historique des accès, ...). L'implication des RSSI s'inscrit également et de façon plus généralisée encore en vertu de la conformité légale en matière de droit des données personnelles.

Sécurité et conformité au droit des données personnelles

Envisagée sous l'angle de la conformité, la sécurité constitue la nouvelle pierre angulaire de la protection des données à caractère personnel par le futur Règlement, eu égard au principe de responsabilité (« accountability »)[4]. Concrètement, la conformité au Règlement s'appréciera eu égard aux mesures et procédures de protection mises en œuvre, leur efficacité devant s'inscrire dans la durée. A l'instar des préconisations des normes ISO (27001 notamment), la conformité impose de tenir une documentation dédiée et régulièrement mise à jour, de prendre des mesures de sécurité adaptées au niveau de risque du traitement des données, de réaliser préalablement une analyse d'impact sur la protection des données (« Privacy Impact Assesment »), de respecter les obligations déclaratives auprès de l'Autorité de contrôle (si requises comme pour le transfert de données hors UE), et de désigner un délégué à la protection des données (sous réserve ces conditions posées). Ainsi, le niveau de sécurité doit impérativement être mis en œuvre à l'issue d'une évaluation des risques qui constitue le préalable à la mise en place des mesures de sécurité techniques et organisationnelles même si cette règle n'apparaît pas dans le texte. Toutefois, en raison de l' « accountability », la preuve de

[4] Sur l'accountability, v. Eric A. Caprioli et Isabelle Cantero, De la sécurité de l'information à la mise en oeuvre du principe d'accountability, Mag-Securs n°39, p.19-21.

cette évaluation antérieure devra être apportée en cas de problème. La sécurité implique que l'on adopte des règles internes et que l'on applique des mesures adaptées. On pense également ici à la Politique de sécurité de l'information et à ses directives d'application pour de domaines plus particuliers (externalisation, BYOD, médias sociaux, etc.) ainsi bien sûr qu'aux documents (chartes informatiques) qui encadrant les différents utilisateurs (salariés, administrateurs, prestataires, etc.). C'est à ce stade que l'on retrouve la protection des données dès la conception (« privacy by design »), ainsi que par défaut (« privacy by default »), que doivent intégrer ces règles internes.

Le principe d'« Accountability » impose l'élaboration d'une politique de sécurité dont il est précisé qu'elle doit tenir compte de l'analyse d'impact des traitements sur la vie privée (pour les traitements « à risque », conformément à l'article 33 de la proposition). Ladite politique doit notamment inclure « *la capacité de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement des données à caractère personne* » (Art. 30-1Bis (b)). Ce principe impose également la mise en place d'une « *procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des politiques, des procédures et des plans de sécurité mis en place pour assurer une efficacité constante* ». Force est de constater que l'évaluation ou l'analyse des risques bien connue des RSSI dans le cadre des systèmes d'information devient le préalable indispensable et nécessaire aux Délégués à la Protection des Données pour apprécier la licéité d'un traitement et in fine s'inscrire en conformité avec la réglementation applicable. Cette démarche et plus globalement toutes les procédures liées au principe de responsabilité confirment le rapprochement entre les deux métiers : DPD et RSSI. D'ailleurs, l'analyse de risques était déjà obligatoire dans certains domaines d'activité comme dans le secteur bancaire et financier (règlement 97-02). Cela est d'autant plus vrai que la CNIL reprend et développe l'intérêt de cette approche dans son Guide « sécurité » publié en 2012, intitulé « *Gérer les risques sur les libertés et la vie privée* »[5].

Ainsi, l'accent mis sur la sécurité pour la protection des données offre au Responsable de la sécurité des systèmes d'information un rôle important à jouer à côté du Délégué à la Protection des Données quant à l'élaboration et à la mise en place des outils et des procédures associées à « l'accountability ». Dès lors, le RSSI pourrait aisément devenir un incontournable interlocuteur ou un acteur de la conformité légale des traitements mis en œuvre au sein de l'entreprise. ■

[5] Guide de la CNIL, édition 2012 (Méthode EBIOS).